Listing of Claims:

1. (Currently amended) A method of using a portable computing device to authenticate ~~authenticating~~ a user [[at]] to use an un-trusted computing system to access user data on the portable computing device ~~the user having at least one portable computing device coupled to a peripheral device~~, the method comprising:

randomly generating, on ~~a temporary password by~~ the portable computing device, a temporary password for controlling access to the user data on the portable computing device;

setting a time limit of less than one minute for the temporary password to remain valid;

sending the temporary password from the portable computing device to ~~the~~ a peripheral device coupled to the portable computing device;

rendering the temporary password by the peripheral device for perception by the user;

~~inputting~~ receiving a user-inputted password~~, by the user, into~~ at the un-trusted computing system;

after receiving~~, by the portable computing device,~~ the user-inputted password ~~input by the user~~ at the un-trusted computing system, sending the user-inputted password from the un-trusted computing system to the portable computing device;

determining, at the portable computing device, whether the user-inputted password matches the temporary password;

determining, at the portable computing device, whether the time limit has been exceeded; and

allowing the user to access [[to]] the user data on the portable computing device ~~using~~ via the un-trusted computing system ~~when~~ in response to determinations that the temporary password matches the user-inputted password and the time limit has not been exceeded.

2. (Original) The method of claim 1, wherein randomly generating the temporary password comprises randomly generating the temporary password periodically.

3. (Original) The method of claim 1, wherein randomly generating the temporary password comprises randomly generating the temporary password in response to a user-initiated action to the peripheral device.

4. (Cancelled)

6. (Original) The method of claim 1, wherein sending the temporary password to the peripheral device comprises sending the temporary password from the portable computing device to the peripheral device over a secure wireless link.

7. (Original) The method of claim 1, wherein rendering the temporary password comprises displaying the temporary password on a display of the peripheral device.

8. (Original) The method of claim 7, further comprising displaying a number of seconds until the temporary password expires on a display of the peripheral device.

9. (Original) The method of claim 1, wherein rendering the temporary password comprises rendering the temporary password audibly for hearing by the user.

10. (Original) The method of claim 1, wherein the password comprises at least one of numbers, letters, symbols, images, and shapes.

11. (Original) The method of claim 1, further comprising detecting initiation of an action by the user to the peripheral device to cause the rendering of the temporary password.

12. (Currently amended) The method of claim 1, further comprising:

generating an indicator by the portable computing device;

sending the indicator to the peripheral device and to the un-trusted computing system;

rendering the indicator by the peripheral device for perception by the user;

rendering the indicator by the un-trusted computing system for perception by the user;

determining, by the user, whether the indicator rendered by the peripheral device matches the indicator rendered by the un-trusted computing system;

wherein the user inputs a password only when the indicator rendered by the peripheral device matches the indicator rendered by the un-trusted computing system the user desires to use.

13. (Original) The method of claim 1, wherein the peripheral device is at least one of worn by the user and carried by the user.

14. (Original) The method of claim 1, wherein the portable computing device and the un-trusted computing system communicate over a wireless link.

15. (Currently amended) An article comprising:

a computer readable storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions ~~provide for authenticating a user of an un-trusted computing system, the user having at least one portable computing device coupled to a peripheral device, by randomly generating a temporary password by the portable computing device, by sending the temporary password to the peripheral device, by receiving at the portable computing device a password input by the user from the un-trusted computing system, and by allowing access to the portable computing device using the un-trusted computing system when the temporary password matches the user-inputted password~~

cause execution of operations comprising:

randomly generating, on a portable computing device, a temporary password for controlling access to user data on the portable computing device;

setting a time limit of less than one minute for the temporary password to remain valid;

sending the temporary password from the portable computing device to a peripheral device coupled to the portable computing device;

rendering the temporary password by the peripheral device for perception by a user;

receiving a user-inputted password at the un-trusted computing system;

after receiving the user-inputted password at the un-trusted computing system, sending the user-inputted password from the un-trusted computing system to the portable computing device;

determining, at the portable computing device, whether the user-inputted password matches the temporary password;

determining, at the portable computing device, whether the time limit has been exceeded; and

allowing the user to access the user data on the portable computing device ~~using~~ via the un-trusted computing system in response to determinations that the temporary password matches the user-inputted password and the time limit has not been exceeded.

16. (Original) The article of claim 15, wherein instructions for randomly generating the temporary password comprise instructions for randomly generating the temporary password periodically.

17. (Cancelled)

19. (Original) The article of claim 15, wherein instructions for sending the temporary password to the peripheral device comprise instructions for sending the temporary password from the portable computing device to the peripheral device over a secure wireless link.

20. (Original) The article of claim 15, wherein the password comprises at least one of numbers, letters, symbols, images, and shapes.

21. (Currently amended) A system for authenticating a user desiring to use an un-trusted computing system comprising:

an un-trusted computing system;

a portable computing device operable to communicate with the un-trusted computing system; and

a peripheral device, coupled to the portable computing device, capable of rendering a password for perception by the user;

the portable computing device comprising:

a random password generator to randomly generate a temporary password for controlling access to user data on the portable computing device;

a memory to store instructions and the user data; and

a processor to execute the instructions obtained from the memory to set a time limit of less than one minute for the temporary password to remain valid, to send the temporary password to the peripheral device for rendering to the user, to receive from the un-trusted computing system a ~~password input by the user;~~ user-inputted password, to determine whether the user-inputted password matches the temporary password, to determine whether the time limit has been exceeded, and to allow the user to access [[to]] the user data on the portable computing device [[by]] via the un-trusted computing system ~~when~~ in response to determinations that the temporary password matches the user-inputted password and the time limit has not been exceeded.

22. (Original) The system of claim 21, wherein the peripheral device comprises a display and renders the password by displaying the password on the display.

23. (Original) The system of claim 21, wherein the portable computing device communicates with the peripheral device over a secure wireless link.

24. (Original) The system of claim 21, wherein the portable computing device communicates with the un-trusted computing system over a wireless link.

25. (Original) The system of claim 21, wherein the random password generator randomly generates the temporary password periodically, the temporary password valid for only a predetermined period of time.

26. (Original) The system of claim 21, wherein the peripheral device is capable of being at least one of worn and carried by the user.

27. (Original) The system of claim 21, wherein the peripheral device comprises an input mechanism activation of which initiates rendering of the password by the peripheral device.

28. (Original) The system of claim 21, wherein the peripheral device comprises an input mechanism activation of which causes the portable computing device to randomly generate a new temporary password.